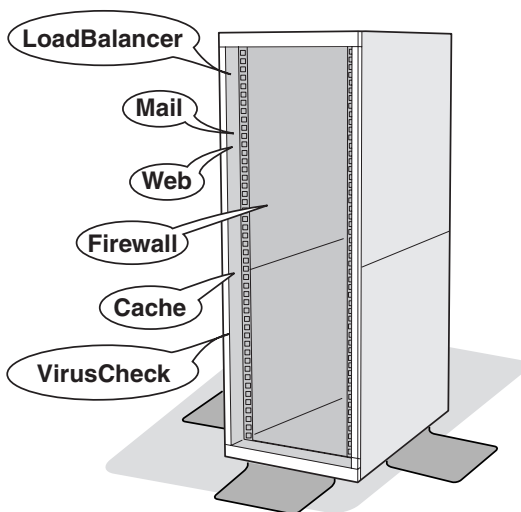
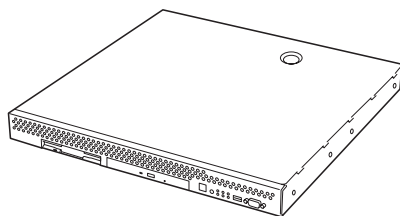
1 知っておきたいこと

本製品や添付のソフトウェアの特長、導入の際に知っておいていただきたい事柄について説明します。

インターネットアプライアンスサーバについて

お買い求めになられたインターネットアプライアンスサーバ「Express5800/FirewallServer」について説明します。

インターネットアプライアンスサーバとは

「オール・イン・ワン」から「ビルドアップ」へ。
インターネットビジネスやデータセンタサーバ化社会において大量のデータを高速に処理するために開発されたのが、「インターネットアプライアンスサーバ」です。
お使いになる環境や用途に応じて必要となる機能を備えたサーバを追加することでシステムをビルドアップすることができます。

1台のラックにそれぞれの機能を持つサーバを搭載

インターネットアプライアンスサーバの主な特長と利点は次のとおりです。

- **省スペース**

  すべてのモデルに厚さ1U（ユニット）のコンパクトな筐体を採用。

- **運用性**

  運用を容易にする管理ツール。

- **クイックスタート**

  ウィザード形式の専用設定ツールを標準装備。短時間（約30分）でセットアップを完了します。

- **高い信頼性**

  単体ユニットに閉じた動作環境で単機能を動作させるために、障害発生の影響は個々のユニットに抑えられます。また、絞り込まれた機能のみが動作するため、万一の障害発生時の原因の絞り込みが容易です。

- **コストパフォーマンスの向上**

  専用サーバに最適なチューニングが行えるため、単機能の動作において高い性能を確保できます。また、単機能動作に必要な環境のみ提供できるため、余剰スペックがなく低コスト化が実現されます。

- **管理の容易性**

  環境設定や運用時における管理情報など、単機能が動作するに必要な設定のみです。そのため、導入・運用管理が容易に行えます。

インターネットアプライアンスサーバファミリーには、目的や用途に応じて次のモデルが用意されています。

- FirewallServer

  インターネットと接続した企業ネットワークを外部からの不正なアクセスから守るファイアウォール専門のサーバです。

- MailWebServer

  WebやFTPのサービスやインターネットを利用した電子メールの送受信や制御などインターネットサーバとしての必要となるサービスを提供するサーバです。

- CacheServer

  Webアクセス要求におけるプロキシサーバでのヒット率の向上(Foward Proxy)やWeb(情報発信)サーバからダウンロードしたデータのキャッシングによるアクセス要求へのレスポンスを向上、Webサーバの負荷軽減(Reverse Proxy)を目的としたサーバです。

- LoadBalancer

  複数台のWebサーバへのトラフィック(要求)を整理し、負荷分散によるレスポンスの向上を目的としたサーバです。

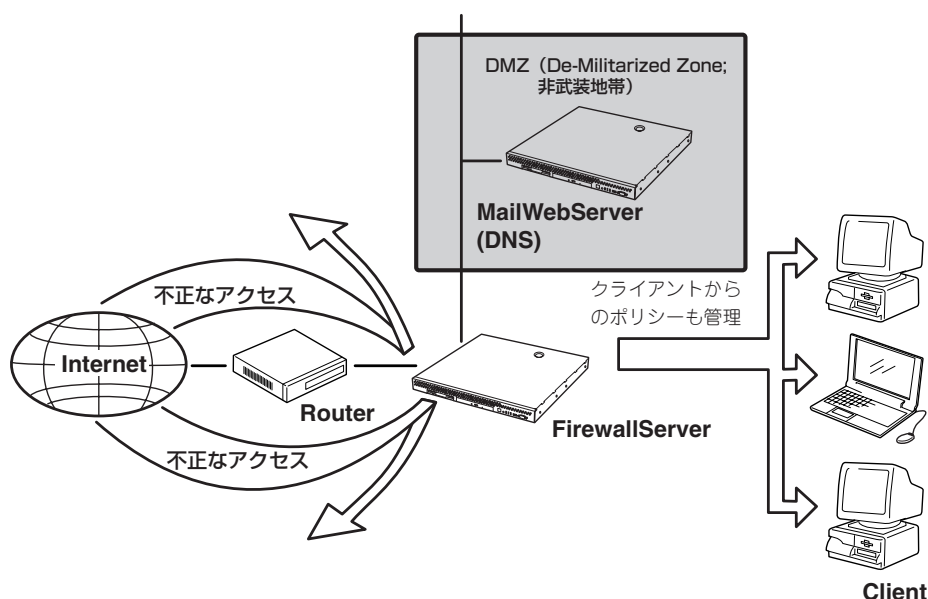
- VirusCheckServer

  インターネット経由で受け渡しされるファイル(電子メール添付やファイルダウンロード)から各種ウィルスを検出/除去し、オフィスへのウィルス侵入、外部へのウィルス流出を防ぐことを目的としたサーバです。

特長と機能

特長や機能について説明します。

概　要

FirewallServerはインターネットと接続された企業ネットワークを外部からの不正なアクセスから守ることが可能なファイアウォール・アプライアンス製品です。
ファイアウォールエンジンとして、Check Point Software Technologies社のFireWall-1を採用しました。
また、本製品は必要なソフトウェアがすべてプリインストールされているため短期間での導入／運用が可能です。

Express5800/FirewallServerはFirewallServer本体以外に、以下のハードウェアが必要です。別途ご用意ください。

- **管理用コンピュータ**

  FirewallServerメンテナンス用です。FirewallServerの基本設定などを行います。

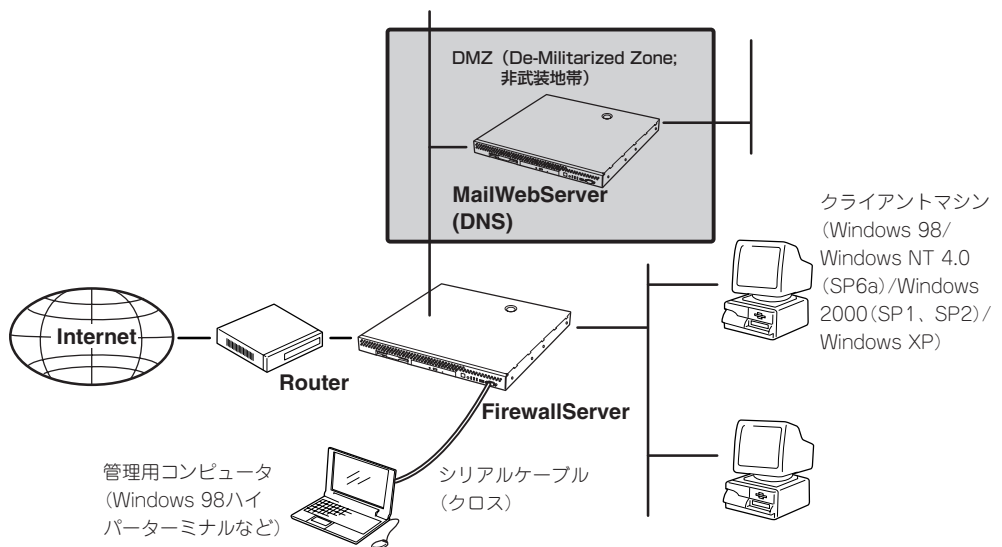
- **シリアルケーブル(クロス)**

  FirewallServerとコンソール用PCの接続に使用します。

- **クライアントマシン**

  FirewallServerのネットワーク上に存在するWindows 98/NT/2000/XPで動作するコンピュータです。FirewallServerへインストールするポリシーを編集したり、ログを見たりする場合に使用します。

ポリシーの編集やログのチェックは専用のユーティリティを使います。ユーティリティをインストールするためには、同梱されているCheck Point Next GenerationのCD-ROMが必要です。用意してください。

以下のような構成になります。

FirewallServerが提供するファイアウォールの特徴は次のとおりです。

- **アクセス制御**
  - あらかじめ定義されている200以上の広範囲なアプリケーション、サービス、プロトコルをアクセス制御可能です。
  - オープン・アーキテクチャの採用と強力なINSPECTスクリプト言語により、新しいアプリケーションやカスタム・アプリケーションに対応するよう拡張することもできます。
  - OSの不要なサービスを削除または停止していることにより高いセキュリティレベルを提供。
- **DMZ（De-Militarized Zone: 非武装地帯）の構築が可能**
  - ネットワークインタフェース4ポート標準装備。
  - 3つ目のネットワークインタフェースに接続した非武装セグメント（DMZ）として利用できます。DMZにはWWWサーバなどの公開サーバを設置します。
- **認証**
  - アクセス制御時の認証機能として、3つの強力な認証方法（ユーザー認証、クライアント認証、セッション認証）と複数の認証方式（S/Key、OS Password、FireWall-1 Password、RADIUS、TACACS）を使用した総合的なユーザー認証をサポートしています。
  - サーバ・アプリケーションやクライアント・アプリケーションをまったく変更することなく、ユーザーの認証が可能です。

- **NAT(ネットワーク・アドレス変換)**

  ー インターネットから内部ネットワーク・アドレスを隠し、インターネット上で公開されることを防止します。

  ー 静的アドレス変換(1対1)モードと動的アドレス変換(複数対1または非表示)モードをサポートしています。

- **直感的で定評のあるグラフィカル・ユーザー・インタフェース**

  セキュリティ・ポリシーの定義、ユーザーの管理、通信の監査や報告などをGUIにより容易に行うことができます。

- **二重化構成が可能**

  フェイルオーバ機能を標準実装しています。FirewallServerを2台使用することでフェイルオーバ(二重化)を実現することができます。

FirewallServerの製品体系

本製品にはFireWall-1のライセンスはバンドルされていません。別途FirewallServerのライセンス製品を購入する必要があります(ただし、30日間だけ使用することが可能な評価用ライセンスが2本バンドルされています)。
FirewallServerの製品体系は大きく以下の3つに分類できます。

- FirewallServer本体(N8100-845)
- FirewallServerライセンス(UL4005-xxx)
- FirewallServerソフトウェアサポートサービス(ULH100-4000-xxx)

以降、これらについて説明します。

ライセンスタイプとノード数

- **ライセンスタイプ**

  FireWall-1にはPermanent License (以降、「ライセンス」と記す)とEvaluation License (以降、「評価ライセンス」と記す)の2つのライセンスタイプがあります。

  FirewallServerには、「評価用ライセンス」のみをバンドルしており「ライセンス」は別途ライセンス製品として用意しています。各「ライセンス」はノード数や機能毎に用意されており、用途毎に適切な「ライセンス」を選び購入いただけます。

- **ノード数の数え方**

  ノードとは、1つのIPアドレスを持つコンピューティング・デバイスのことです。マルチユーザー・コンピュータでもIPアドレスが1つであれば1つのノードとして数えます。FirewallServer(FireWall-1)によって保護されているノード(FirewallServer自身とDMZも含む)は、たとえIPアドレスがプロキシやその他の手段で遮蔽されていたとしてもすべて制限値の数に数えられます。

- **評価用ライセンス**

  FirewallServer本体には評価用ライセンスがバンドルされています。評価用ライセンスはCheck Point Next Generationのメディアに添付されているCertificate Keyで即日入手することができます。評価用ライセンスの有効期限はライセンスを入手してから30日間です。また、1つのkeyから評価用ライセンスを2回入手することができます。

- **評価用ライセンスの入手/インストール方法**

  Check Point User Center(http://www.checkpoint.com/usercenter/)にアクセスし、画面の指示に従って必要事項を入力してください。なお、Certificate Keyには、Check Point Next Generationのメディアのケースに[Certificate Key] と書かれた白いラベルが貼ってありますので、そこに書かれている文字列を入力してください。上記Webでの手続きが完了しますと、登録したアドレス宛にE-mailにてライセンスが通知されます。

評価用ライセンスのインストール方法は基本的に通常のライセンスと同じです。「システムのセットアップ」に従ってください。

評価用ライセンスについてはCheck Point社の都合により、予告なしにその取得方法などが変更になることがあります。あらかじめご了承ください。

FirewallServer本体(N8100-845 Express5800/FirewallServer)

本製品にはライセンスがバンドルされていませんので、別途ライセンス製品を購入する必要があります。

FirewallServerライセンス製品

- **ファイアウォール機能のみのライセンス**

UL4005-201　Exp58/FWS 25ライセンス

UL4005-211　Exp58/FWS 50ライセンス

UL4005-221　Exp58/FWS 100ライセンス

UL4005-231　Exp58/FWS 250ライセンス

UL4005-241　Exp58/FWS 無制限ライセンス

ノード数にあわせて5ライセンス製品を用意しています。VPN機能はありません。

「ライセンス製品の構成例」のAを参照してください。

- **ファイアウォール機能とVPN機能のライセンス**

UL4005-202　Exp58/FWS(VPN機能付) 25ライセンス

UL4005-212　Exp58/FWS(VPN機能付) 50ライセンス

UL4005-222　Exp58/FWS(VPN機能付) 100ライセンス

UL4005-232　Exp58/FWS(VPN機能付) 250ライセンス

UL4005-242　Exp58/FWS(VPN機能付) 無制限ライセンス

ノード数にあわせて5ライセンス製品を用意しています。VPN機能を含んでいます。

- **ファイアウォール機能を二重化構成で使用するためのライセンス**

  UL4005-203　Exp58/FWS二重化パック 25ライセンス

  UL4005-213　Exp58/FWS二重化パック 50ライセンス

  UL4005-223　Exp58/FWS二重化パック100ライセンス

  UL4005-233　Exp58/FWS二重化パック 250ライセンス

  UL4005-243　Exp58/FWS二重化パック 無制限ライセンス

  ノード数にあわせて5ライセンス製品を用意しています。VPN機能はありません。

  ライセンス申請書には、管理サーバとFirewallServer×2のIPアドレスをそれぞれご記入ください。

  それぞれライセンスが発行されるので、対応するサーバに投入してください。

- **ファイアウォール機能とVPN機能を二重化構成で使用するためのライセンス**

  UL4005-204　Exp58/FWS二重化パック(VPN機能付) 25ライセンス

  UL4005-214　Exp58/FWS二重化パック(VPN機能付) 50ライセンス

  UL4005-224　Exp58/FWS二重化パック(VPN機能付) 100ライセンス

  UL4005-234　Exp58/FWS二重化パック(VPN機能付) 250ライセンス

  UL4005-244　Exp58/FWS二重化パック(VPN機能付) 無制限ライセンス

  ノード数にあわせて5ライセンス製品を用意しています。VPN機能の二重化も可能です。

  「ライセンス製品の構成例」のBを参照してください。

  ライセンス申請書に管理サーバとFirewallServer×2のIPアドレスをそれぞれご記入ください。

  それぞれライセンスが発行されるので、対応するサーバに投入してください。

- **機能アップグレードについて**

  ライセンス数のアップグレード、VPN機能の追加、二重化構成へのアップグレード等に関しては、NEC営業・SEへご相談ください。

- **ライセンスキーの取得について**

  FirewallServerを利用するためには、ライセンス製品を購入後に申請を行い、ライセンスキーを取得する必要があります。ライセンス製品に添付されている「FirewallServerライセンス申請書」に必要事項を記入の上、新日鉄ソリューションズ株式会社(NS-Sol)にFAXします。後日(通常5営業日)、E-mailでライセンスキーが送付されます。

ライセンス申請はライセンス製品ご購入後3ヶ月以内に行ってください。それ以降の申請になりますと、手続きに時間がかかることがありますので注意してください。製品の購入からサポートサービス開始までの流れについては後述の「登録の手続き」をご覧ください。

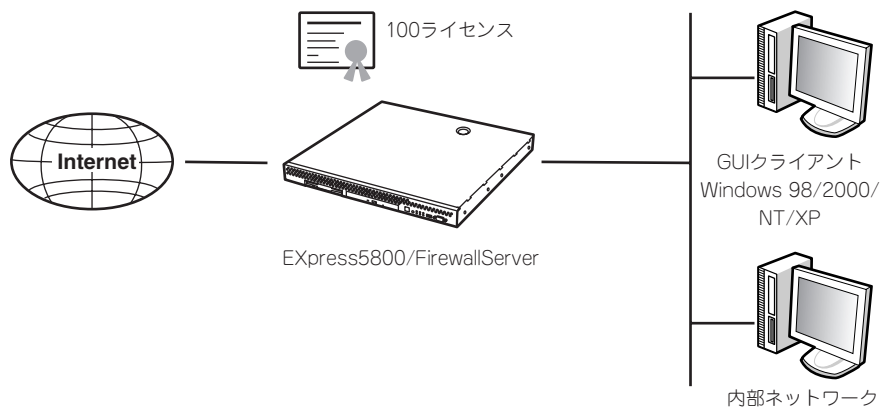
ライセンス製品の構成例

ライセンス製品の組み合わせの例を紹介します。

A. ファイアウォール機能のみを使用する場合(ノード数が51～100の場合の例)

VPN機能、二重化を利用しない場合の組み合わせです。

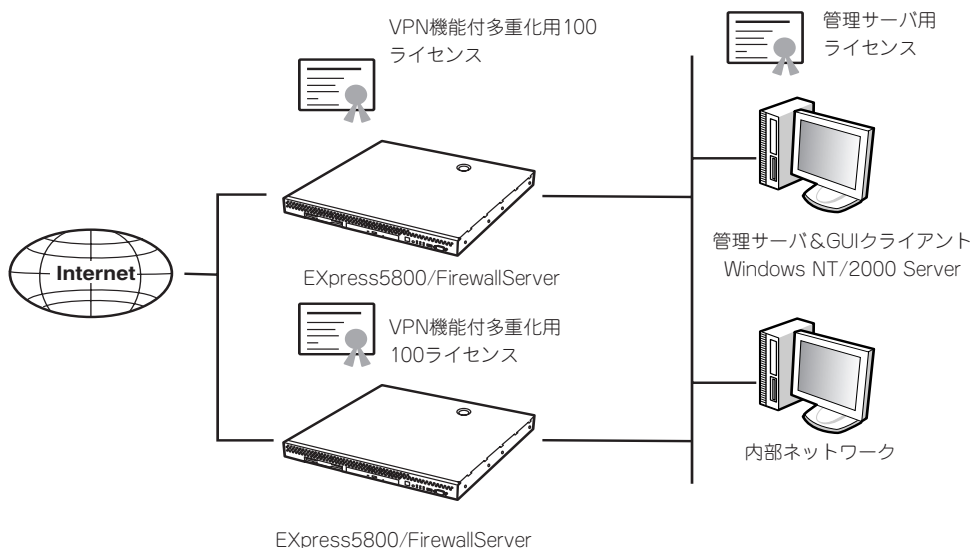
N8100-845　Express5800/FirewallServer　×1

UL4005-221　Exp58/FWS 100ライセンス　×1

B. 二重化構成で、VPN通信も行う場合(ノード数が51～100の場合の例)

FirewallServer2台とExp58/FWS二重化パックを1つ購入することで二重化構成を構築することができます。2台のFirewallServerを管理するための管理モジュールが必要になります。別途管理サーバ(WindowsNT Serverなど)を用意し、このマシンに管理モジュールとそのライセンスをインストールします。

フェイルオーバ機能はFirewallServerに標準搭載のため、二重化のためのソフトウェアを別途購入する必要はありません。

N8100-845　Express5800/FirewallServer　×2

UL4005-224　Exp58/FWS 二重化パック(VPN機能付き)100ライセンス　×1

別途管理サーバが必要となります。
また、ライセンス申請書には、管理サーバとFirewallServerのIPアドレスをそれぞれご記入ください。手配いただくライセンス製品は1本ですが、ライセンスが3つ発行されるのでそれぞれ対応するサーバに投入してください。

ソフトウェアサポートサービス

FirewallServerのソフトウェアについては、ライセンス製品に適合したFirewallServerソフトウェアサポートサービス(以降、サービス製品と記します)を用意しています。
本サービス製品は、イスラエルCheck Point社からのパッチ提供サービスとNECのQ&Aサポートサービスを統合した製品です。本サービスを受けるためには以下の製品の購入が必須となります。
本サービス製品はライセンス製品と1対1で対応していますので、ライセンス製品に適合したサービス製品を購入しなければなりません。

重要 **購入前には必ず型番等についてお問い合わせください。**

- Exp58/FWS(25ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(50ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(100ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(250ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(無制限ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(VPN機能付25ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(VPN機能付50ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(VPN機能付100ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(VPN機能付250ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(VPN機能付無制限ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パック25ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パック50ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パック100ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パック250ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パック無制限ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パックVPN機能付25ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パックVPN機能付50ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パックVPN機能付100ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パックVPN機能付250ライセンス1年間)ソフトウェアサポートサービス
- Exp58/FWS(二重化パックVPN機能付無制限ライセンス1年間)ソフトウェアサポートサービス

上記の他に機能アップグレード用のサービス製品も用意しています。

- **サービス内容**

FirewallSreverのソフトウェアについて、お客様(担当のNEC営業・SEを含む)から電話、E-mailおよびFAXによるNEC窓口への問い合わせを可能にします。

□ 設定や再インストールに関するQ&Aサービス
□ 障害解決のための問題切り分け支援(Q&A)サービス
□ パッチ、サービスパック(ダウンロードを予定)およびバージョンアップ媒体(希望により送付)のサービス

本サービス内容については、FireWall-1/VPN-1開発元のイスラエルCheck Point社のサービスに準拠する部分があり、将来変更される可能性がありますので予めご了承ください。

上記各サービスには、オンサイトでのサービスは含まれておりません。オンサイトでの支援をご希望の場合は、別途、有償にて承りますのでNEC営業・SEまでご連絡ください。

- **サービス受付時間**

NEC営業日 AM9:00～AM12:00、PM1:00～PM5:00

- **問合せ窓口のご案内**

お客様の登録が完了され次第、ご案内します。

- **登録手続き**

本サービスを受けるためには、サービス製品に同梱されている「FirewallServerソフトウェアサポートサービス申請書」(以降、申請書と記す)に必要事項を記入の上、申請書に記載されている宛先新日鉄ソリューションズ(NS-Sol)にFAXします。

本サービス製品を発注いただき上記申請書を送付いただいた後、登録手続きを行います。手続き完了後、NECより登録完了のご案内を送付いたします。本手続きにはイスラエルCheck Point社との契約部分があり、その手続きに時間がかかる場合がありますので予めご了承ください。

重要 **本サービス申請時にはライセンス製品をご購入いただき、既に(評価ライセンスではなく)正式なライセンスの申請・取得が済んでいる必要があります。**

サービス申請シートのCK(Certificate Key)記入欄には、ライセンスを取得したときのE-mail(以下の例)に記述されているCertificate Keyをご記入ください。

CheckPoint Next Generationパッケージに貼られているCertificate Keyは評価用ライセンス取得に必要なもので、本サービスに必要な情報ではありませんのでご注意ください。

例:　ライセンス申請後に送付されるE-mailの内容(一部)

この文字列を登録シートのCK欄に記入

```
  :
Request Details
---------------
Certificate Key:    xxxx xxxx xxxx
Product:            CPFW-EFC-U-NG (FireWall-1 Enterprise Center for unlimited number of
IP address)
Version: NG
  :
```

サポートが開始されるまでの流れは以下のようになります。

1. FirewallServerライセンス製品、ソフトウェアサポートサービス製品を購入する。
2. 暫定サポートサービスへの登録をする(NEC営業・SEが行います)。
3. ライセンスの申請(FAX)をする。
4. (およそ5営業日後)E-mailで(CKを含む)ライセンスキーが送付される。
5. サポートサービスの申請(FAX)をする。
6. サポートサービス登録のご案内が送付される。

↓

サポートの開始

● **暫定サポート**

上記1の発注から6のサポートサービス登録完了のお知らせ送付までの間は、暫定サポートとして対応いたします。ただし、暫定サポートの間は、NEC営業・SE経由でのお問い合わせとなります。また、暫定サポートの期間は開始後最長3ヶ月(登録完了のお知らせ送付まで)です。

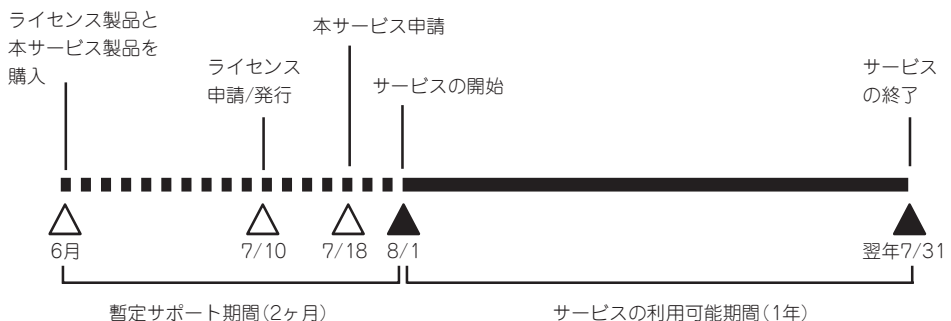
暫定サポートにはオンサイトでのサービスは含まれておりません。オンサイトでの支援をご希望の場合は、別途、有償にて承りますのでNEC営業・SEまでご連絡ください。

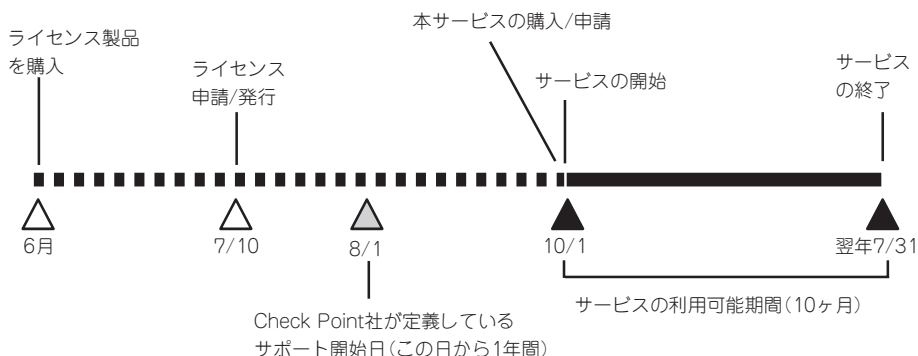
● **サービス期間**

正式なライセンスを申請し、イスラエルCheck Point社がライセンスを発行した日の翌月1日から1年間有効になります。例えば、7月18日に正式なライセンスが発行された場合、8月1日から翌年の7月31日の1年間となります。ただし、8月1日(月はじめの1日)に正式なライセンスが発行された場合は、8月1日から7月31日までの1年間となります。

重要 **本サービス満了日は、(本サービス購入日ではなく)ライセンス発行日が起点になりますのでご注意ください。**

例1 6月はじめにライセンス製品および本サービス製品を購入、本サービス申請を8月1日以前に行った場合。

この場合は、1年間のサポートを受けられます。

例2 6月はじめにライセンス製品を購入・申請、本サービス製品を10月1日に購入・申請した場合。

この場合は、サービスを受けられる期間が短くなります。

例2のようにライセンス申請後しばらくしてから本サービスをご購入になりますと、その間(上記の例2では8/1〜9/30まで)の分のサービスが受けられません。

イスラエルCheck Point社の規定としてサポート締結可能期間はライセンスの発行日から1年間ですが、本サービスの購入・申請が遅れますと上記のようにサービスを受けられる期間が短くなる場合があります。

重要 **本サービスはライセンス申請のタイミングに合わせて速やかにご購入されることを強くお勧めいたします。**

- **ソフトウェアサポートサービスに関する注意**
  - ソフトウェアサポートサービスは以下の条件を満たす場合のみ、ご購入できます。（条件を満たさない場合は、別途ご相談ください。）
    - □ はじめて購入される場合は、正式なライセンス発行日から1年以内
    - □ 2回目以降の購入で、前回の契約満了日から1年以内
  - 購入したFirewallServerライセンス製品と適合するサービスしか購入できません。
  - 本サービスにはイスラエルCheck Point社との契約が含まれますので、いかなる理由でも返品や交換はできません。
  - イスラエルCheck Point社での登録作業で時間がかかる可能性がありますが、本サービス製品を発注・申請書を送付いただいた時点からサポートを開始できます。
  - 機能アップグレード等をする際にはソフトウェアサポートサービスのアップグレードも必須となります。手配方法はNEC営業・SEまでお問い合わせください。

注意・制限事項

本製品はファイアウォール専用のマシンとして使用してください。他の業務用アプリケーションなどをインストールしないでください。

添付のディスクについて

本装置にはセットアップや保守・管理の際に使用するCD-ROMやフロッピーディスクが添付されています。ここでは、これらのディスクに格納されているソフトウェアやディスクの用途について説明します。

重要 **添付のフロッピーディスクやCD-ROMは、システムの設定が完了した後でも、システムの再インストールやシステムの保守・管理の際に使用する場合があります。なくさないように大切に保存しておいてください。**

- **OS CD-ROM**

  Linuxオペレーティングシステムが格納されているCD-ROMです。再インストールの際は、初めにこのCD-ROMを使用します。

- **バックアップCD-ROM**

  システムのバックアップとなるCD-ROMです。

  バックアップCD-ROMには、システムのセットアップに必要なソフトウェアや各種モジュールが格納されています。

- **Check Point Next Generation(CD-ROM)**

  ファイアウォールエンジンであるCheck Point Software Technologies社の「FireWall-1」を格納したCD-ROMです。

- **保守・管理ツールCD-ROM**

  本体およびシステムの保守・管理の際に使用するCD-ROMです。

  このCD-ROMには次のようなソフトウェアが格納されています。

  - 保守・管理ツール

    再セットアップの際に装置の維持・管理を行うためのユーティリティを格納するためのパーティション(保守パーティション)を作成したり、システム診断やオフライン保守ユーティリティなどの保守ツールを起動したりするときに使用します。詳細は5章を参照してください。

  - MWA

    システムが立ち上がらないようなときに、リモート(LAN接続またはRS-232Cケーブルによるダイレクト接続)で管理コンピュータから本装置を管理する時に使用するソフトウェアです。詳細は5章を参照してください。

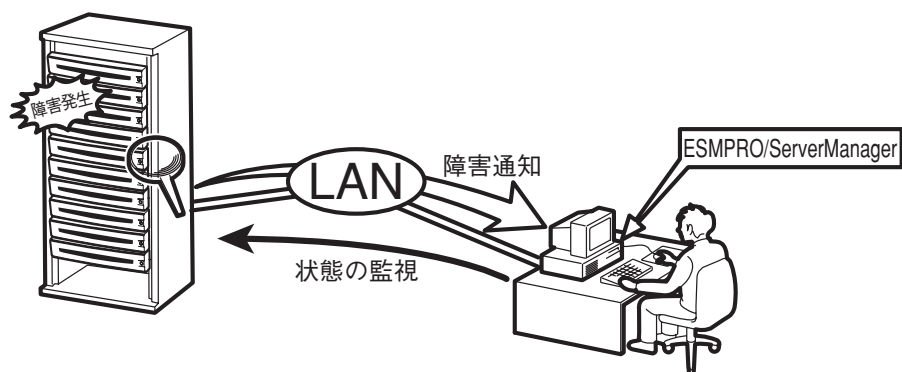
  - ESMPRO/ServerManager

    ESMPRO/ServerAgentがインストールされたコンピュータを管理します。詳細は6章を参照してください。

- **再インストール用ディスク(フロッピーディスク)**

  再インストールの際に使用するキーディスクです。なくさないよう、大切に保管しておいてください。

ESMPRO

「ESMPRO®」は、NECが提供するサーバ管理・監視ソフトウェアです。
システムの稼動状況や障害の監視をリモートで行い、障害を事前に防ぐことや万一の場合に迅速に対応することができます。

本装置を運用する際は、ESMPROを利用して、万一のトラブルからシステムを守るよう心がけてください。
添付のCD-ROM「バックアップCD-ROM」にはシステムを監視するソフトウェア「ESMPRO/ServerAgent」が格納されています。ESMPRO/ServerAgentがインストールされたシステムを管理するためのソフトウェア「ESMPRO/ServerManager」は「保守・管理ツールCD-ROM」に格納されています。
ESMPRO/ServerAgentはあらかじめシステムの一部として装置に組み込まれています。また、再インストールの際にも自動的にインストールされます。
ESMPRO/ServerManagerはネットワーク上のコンピュータにインストールします。
ESMPRO/ServerAgentとESMPRO/ServerManagerの詳細は、6章を参照してください。

ESMPROを使ってさらに高度なクライアントサーバシステムを構築する場合は別売の「ESMPROシステム構築ガイド Ver.2.0（UL9005-201）」を参照してください。この説明書はESMPRO製品を活用するためのガイドです。

また、ESMPROには、サーバ管理用ソフトウェアをはじめ、ネットワーク管理や電源管理、ストレージ管理を行う専用のアプリケーション（ESMPROプロダクト）が用意されています。ESMPROプロダクトについては、お買い求めの販売店または保守サービス会社にお問い合わせください。

各部の名称と機能

本体の各部の名称を次に示します。ここでは本装置で使用するコネクタやランプのみを説明します。

本体前面

<フロントベゼルを取り外した状態>

① **フロントベゼル**

日常の運用時に前面のデバイス類を保護するカバー。添付のセキュリティキーでロックすることができる(→22ページ)。

② **キースロット**

フロントベゼルのロックを解除するセキュリティキーの差し口。

③ **POWERランプ(緑色)**

電源をONにすると緑色に点灯する(→20ページ)。

④ **STATUSランプ(緑色/アンバー色)**

本体の状態を表示するランプ。正常に動作している間は緑色に点灯する。異常が起きると緑色に点滅、またはアンバー色に点灯/点滅する(→20ページ)。

⑤ **DISK ACCESSランプ(緑色)**

取り付けているディスクが動作しているときに点灯する(→25ページ)。

⑥ **UID(ユニットID)ランプ(黄色)**

装置を識別するためのランプ(→20ページ)。ランプ点灯中をメンテナンス中とした場合、本体前面/背面からメンテナンス中の装置を見分けることができる。

⑦ **ACT/LINKランプ(緑色)**

ネットワークポートが接続しているハブなどのデバイスとリンクしているときに緑色に点灯し、アクティブな状態にあるときに緑色に点滅する(→21ページ)。丸数字の後の数字は「1」がLANポート1(標準LAN)用のランプで、「2」がLANポート2(拡張LAN)用のランプを示す。

⑧ **3.5インチフロッピーディスクドライブ**

3.5インチフロッピーディスクを挿入して、データの書き込み/読み出しを行う装置(→25ページ)。

⑧-1 ディスクアクセスランプ

⑧-2 ディスク挿入口

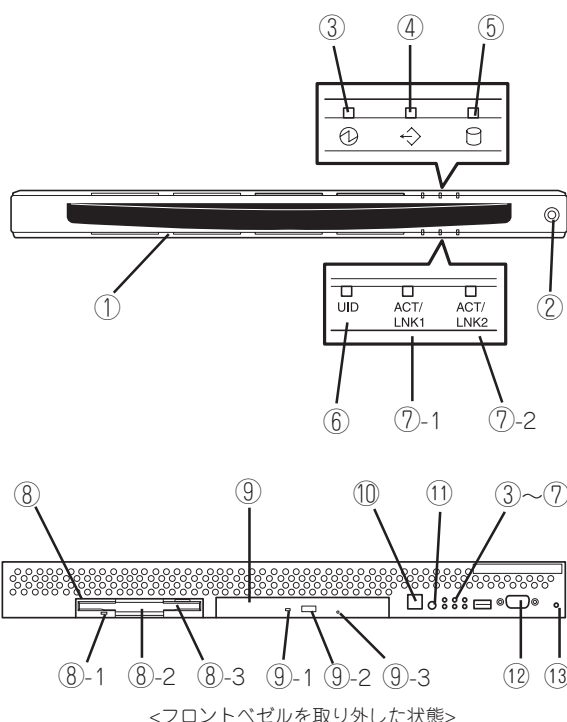
⑧-3 イジェクトボタン

⑨ **CD-ROMドライブ**

CD-ROMの読み出しを行う装置(→27ページ)。

⑨-1 ディスクアクセスランプ

⑨-2 CDトレーイジェクトボタン

⑨-3 エマージェンシーホール

⑩ **POWERスイッチ**

電源をON/OFFするスイッチ(→23ページ)。一度押すとPOWERランプが点灯し、ONの状態になる。もう一度押すと電源をOFFにする。4秒以上押し続けると強制的にシャットダウンする。

⑪ **UID(ユニットID)スイッチ**

本体前面/背面にあるUIDランプをON/OFFするスイッチ。スイッチを一度押すと、UIDランプが点灯し、もう一度押すと消灯する(→24ページ)。

⑫ **シリアルポート2(COM2)コネクタ**

管理コンピュータと接続するためのコネクタ。セットアップと保守の際に使用する。

⑬ **DUMPスイッチ**

押すとメモリダンプを実行する。通常は使用しない。

本体背面

① **シリアルポート1(COM1)コネクタ**

シリアルインタフェースを持つ装置と接続する(→47ページ)。

② **LANコネクタ**

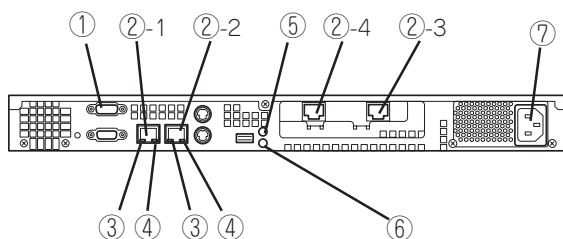
100BASE-TX/10BASE-Tと接続するコネクタ(→47ページ)。LAN上のネットワークシステムと接続する。丸数字の後の数字は次のとおり。

②-1　LANポート1(内部ネットワーク接続用)
②-2　LANポート2(外部ネットワーク接続用)
②-3　LANポート3(DMZネットワーク接続用)
②-4　LANポート4(DMZネットワーク拡張接続用)

③ **ACT/LINKランプ(緑色)**

ネットワークポートが接続しているハブなどのデバイスとリンクしているときに緑色に点灯し、アクティブな状態にあるときに緑色に点滅する(→21ページ)。

④ **100TXランプ(黄色)**

ネットワークポートが100Mbpsで動作しているときに黄色に点灯する。10Mbpsで動作しているときは消灯する(→21ページ)

⑤ **POWERランプ(緑色)**

電源をONにすると緑色に点灯する(→20ページ)。

⑥ **UID(ユニットID)ランプ(黄色)**

本体を識別するためのランプ(→20ページ)。ランプ点灯中をメンテナンス中とした場合、本体前面/背面からメンテナンス中の装置を見分けることができる。

⑦ **電源コネクタ**

添付の電源コードを接続する(→47ページ)。

装置内部

① ハードディスクベイ(ハードディスクを搭載済み)

② 冷却ファン(丸数字の後の数字はファン番号を示す)

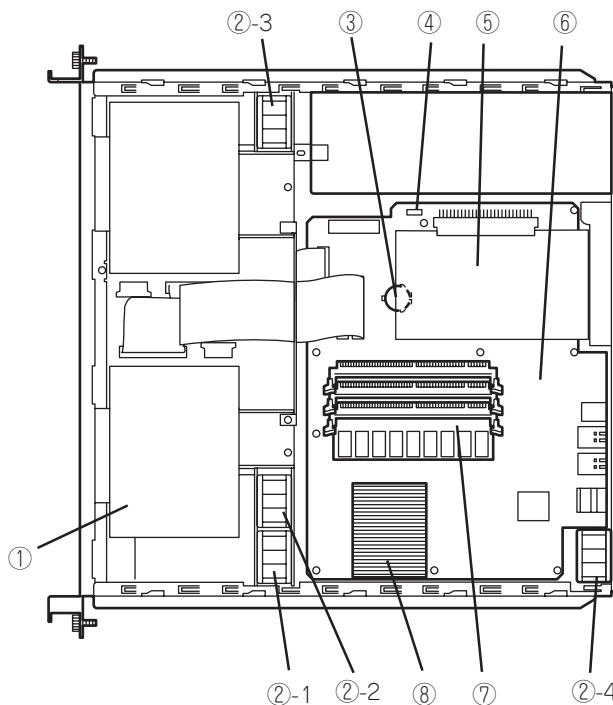
③ リチウム電池

④ コンフィグレーションジャンパ

⑤ ネットワークカード

⑥ マザーボード

⑦ DIMM(右図の下からDIMM #1→DIMM #2→DIMM #3, Slot #1に1枚標準装備)

⑧ プロセッサ(CPU)

ランプ

本体前面には8つ、背面には6つのランプがあります。ランプの表示とその意味は次のとおりです。

POWERランプ(⏻)

本体前面と背面に各1個あります。電源がONの間、ランプが緑色に点灯しています。

STATUSランプ(⟡)

本体前面にあります。本体が正常に動作している間はSTATUSランプは緑色に点灯します。STATUSランプが消灯しているときや、緑色に点滅、またはアンバー色に点灯/点滅しているときは本体になんらかの異常が起きたことを示します。
異常が起きたときは保守サービス会社に連絡してください。

- ESMPROまたはオフライン保守ユーティリティをインストールしておくとエラーログを参照することで故障の原因を確認することができます。
- いったん電源をOFFにして再起動するときに、OSからシャットダウン処理ができる場合はシャットダウン処理をして再起動してください。シャットダウン処理ができない場合はPOWERスイッチを使った強制電源切断をするか(23ページ参照)、一度電源コードを抜き差しして再起動させてください。

DISK ACCESSランプ(⌸)

本体前面にあります。DISK ACCESSランプは本体内蔵のハードディスクやCD-ROMドライブにアクセスしているときに点灯します。

UID(ユニットID)ランプ

本体前面と背面に各1個あります。本体前面にあるUIDスイッチを押すと点灯しもう一度押すと消灯します。複数台の装置がラックに搭載された中から特定の装置を識別したいときなどに使用することができます。特にラック背面からのメンテナンスのときは、このランプを点灯させておくと、対象装置を間違えずに作業することができます。

ACT/LINKランプ(ACT/LNK1、ACT/LNK2)

本体前面と背面(LANコネクタ1/2部分)に各2個あります。本体標準装備のネットワークポートの状態を表示します。本体とHUBに電力が供給されていて、かつ正常に接続されている場合に点灯します(LINK)。ネットワークポートが送受信を行っているときに点滅します(ACT)。
LINK状態なのにランプが点灯しない場合は、ネットワークケーブルやケーブルの接続状態を確認してください。それでもランプが点灯しない場合は、ネットワーク(LAN)コントローラが故障している場合があります。お買い求めの販売店または保守サービス会社に連絡してください。

アクセスランプ

本体前面にあるフロッピーディスクドライブとCD-ROMドライブのアクセスランプは、それぞれにセットされているディスクやCD-ROMにアクセスしているときに点灯します。

100TXランプ

本体背面のLANコネクタ1/2部分に各1個あります。本体標準装備のネットワークポートの通信モードが100BASE-TXか、10BASE-Tのどちらのネットワークインタフェースで動作されているかを示します。点灯しているときは、100BASE-TXで動作されていることを示します。消灯しているときは、10BASE-Tで動作していることを示します。

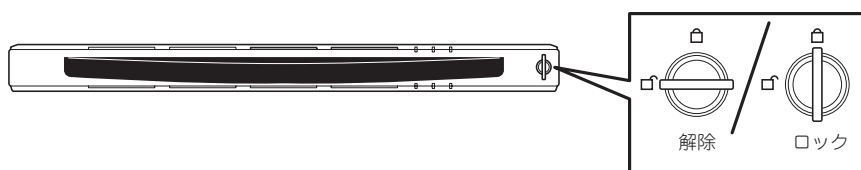
運用時の操作

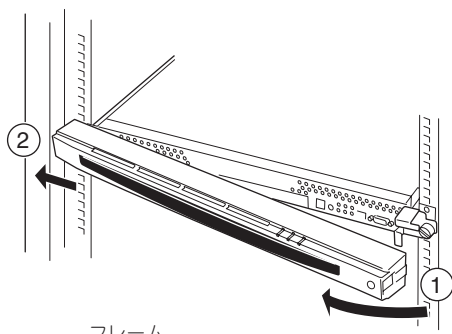
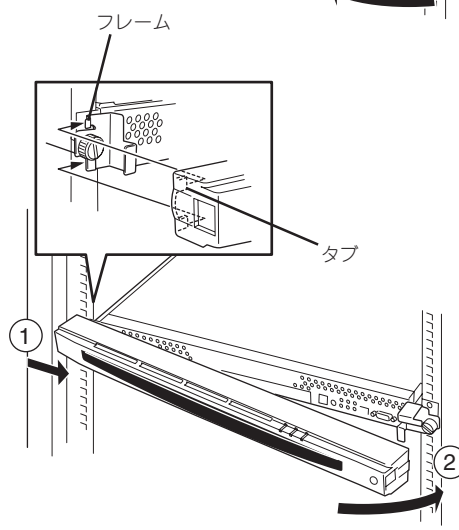
電源のON/OFFの方法など日常の運用で知っておいていただきたい操作手順について説明します。

フロントベゼル　～取り付け・取り外し～

ラックに搭載した本体の電源のON/OFFやフロッピーディスクドライブ、CD-ROMドライブを取り扱うときはフロントベゼルを取り外します(卓上に設置した場合は、フロントベゼルを取り付けることはできません)。

重要 **フロントベゼルは、添付のセキュリティキーでロックを解除しないと開けることができません。**

1. キースロットに添付のセキュリティキーを差し込み、キーをフロントベゼル側に軽く押しながら回してロックを解除する。

2. フロントベゼルの右端を軽く持って手前に引く。

3. フロントベゼルを左に少しスライドさせてタブをフレームから外して本体から取り外す。

フロントベゼルを取り付けるときは、フロントベゼルの左端のタブを本体のフレームに引っかけるようにしながら取り付けます。取り付けた後はセキュリティのためにもキーでロックしてください。

POWERスイッチ　～電源のON/OFF/再起動～

電源は前面にあるPOWERスイッチを押すとONの状態になります。
次の順序で電源をONにします。

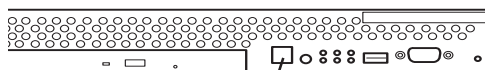
1. ラックに搭載している場合は、フロントベゼルを取り外す。

2. フロッピーディスクドライブにフロッピーディスクをセットしていないことを確認する。

3. 本装置に接続している周辺機器の電源をONにする。

チェック

無停電電源装置(UPS)などの電源制御装置に電源コードを接続している場合は、電源制御装置の電源がONになっていることを確認してください。

4. 本体前面にあるPOWERスイッチを押す。

ヒント

電源コードを接続するとハードウェアの初期診断を始めます(約5秒間)。初期診断中はPOWERスイッチは機能しません。電源コードの接続直後は、約5秒ほど時間をおいてからPOWERスイッチを押してください。

電源をONにしてからしばらくの間、自己診断プログラム(POST)を実行して本装置自身の診断をしています。POSTを完了するとシステムが起動します(約2分で起動します)。
ポリシーがインストールされていれば、そのままファイアウォールとして機能します。

電源のOFFは、管理用コンピュータ(コンソール)を本体のシリアルポート2(COM2)に接続し、rootでログインしてから、shutdownコマンドを実行します。

```
# shutdown -h now
```

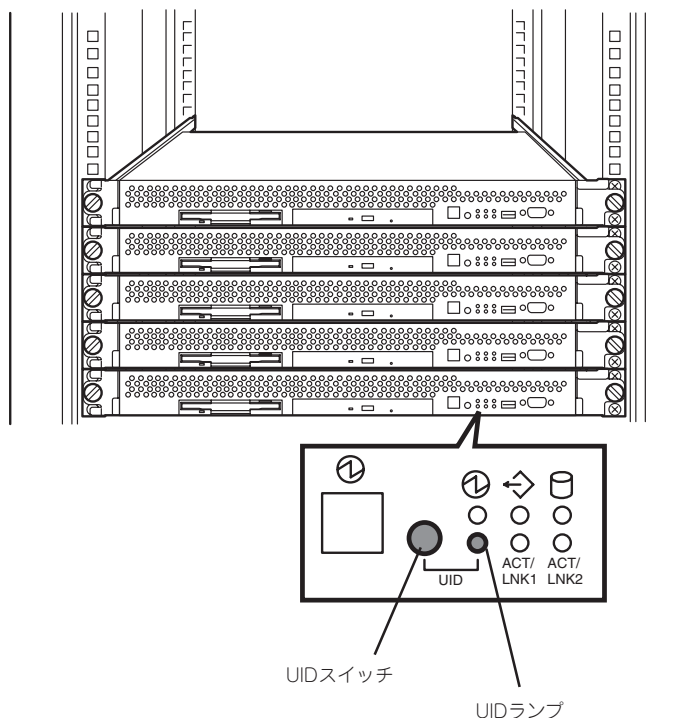
シャットダウン処理の後、自動的に電源がOFFになります。

再起動をする際もコンソールを本体に接続し、rootでログインしてから、shutdownコマンドを実行します。

```
# shutdown -r now
```

約3分でシステムが再起動します。
shutdownコマンドで電源をOFFにできないときは、前面のPOWERスイッチを押してください。それでも電源がOFFにならない場合は、POWERスイッチを4秒以上押し続けてください。システムが強制的に電源OFFとなります。

UID(ユニットID)スイッチ　～サーバの確認～

複数の装置を1つのラックに搭載している場合、保守をしようとしている装置がどれであるかを見分けるために本体の前面および背面には「UID(ユニットID)ランプ」がもうけられています。

前面にあるUID(ユニットID)スイッチを押すとUIDランプが点灯します。もう一度押すとランプは消灯します。
ラック背面からの保守は、暗く、狭い中での作業となり、正常に動作している装置の電源やインタフェースケーブルを取り外したりするおそれがあります。UIDスイッチを使って保守する装置を確認してから作業をすることをお勧めします。

本体背面にもPOWERランプがあります。通電中であるかどうかを確認することができます。

フロッピーディスクドライブ

本体前面にフロッピーディスクを使ったデータの読み出し（リード）・保存（ライト）を行うことのできる3.5インチフロッピーディスクドライブが搭載されています。
本装置では3.5インチの2HDフロッピーディスク（1.44Mバイト）を使用することができます。

フロッピーディスクのセット/取り出し

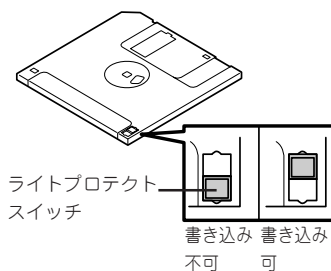
フロッピーディスクをフロッピーディスクドライブにセットする前に本体の電源がON（POWERランプ点灯）になっていることを確認してください。
フロッピーディスクをフロッピーディスクドライブに完全に押し込むと「カチッ」と音がして、フロッピーディスクドライブのイジェクトボタンが少し飛び出します。
イジェクトボタンを押すとセットしたフロッピーディスクをフロッピーディスクドライブから取り出せます。

- フロッピーディスクをセットした後に本体の電源をONにしたり、再起動するとフロッピーディスクから起動します。フロッピーディスク内にシステムがないと起動できません。
- フロッピーディスクアクセスランプが消灯していることを確認してからフロッピーディスクを取り出してください。アクセスランプが点灯中に取り出すとデータが破壊されるおそれがあります。

フロッピーディスクの取り扱いについて

フロッピーディスクが壊れると保存されているデータが使えなくなります。次の点に注意して取り扱ってください。

- フロッピーディスクドライブにはていねいに奥まで挿入してください。
- ラベルは正しい位置に貼り付けてください。
- 鉛筆やボールペンで直接フロッピーディスクに書き込んだりしないでください。
- シャッタを開けないでください。
- ゴミやほこりの多いところでは使用しないでください。
- フロッピーディスクの上に物を置かないでください。
- 直射日光の当たる場所や暖房器具の近くなど温度の高くなる場所には置かないでください。
- たばこの煙に当たるところには置かないでください。
- 水などの液体の近くや薬品の近くには置かないでください。
- 磁石など磁気を帯びたものを近づけないでください。
- クリップなどではさんだり、落としたりしないでください。
- 磁気やほこりから保護できる専用の収納ケースに保管してください。

- フロッピーディスクは、保存している内容を誤って消すことのないようにライトプロテクト(書き込み禁止)ができるようになっています。ライトプロテクトされているフロッピーディスクは、読み出しはできますが、ディスクのフォーマットやデータの書き込みができません。重要なデータの入っているフロッピーディスクは、書き込み時以外はライトプロテクトをしておくようお勧めします。3.5インチフロッピーディスクのライトプロテクトは、ディスク裏面のライトプロテクトスイッチで行います。

- フロッピーディスクは、とてもデリケートな記憶媒体です。ほこりや温度変化によってデータが失われることがあります。また、オペレータの操作ミスや装置自身の故障などによってもデータを失う場合があります。このような場合を考えて、万一に備えて大切なデータは定期的にバックアップをとっておくことをお勧めします。(本製品に添付されているフロッピーディスクは必ずバックアップをとってください。)

CD-ROMドライブ

本体前面にCD-ROMドライブがあります。CD-ROMドライブはCD-ROM（読み出し専用のコンパクトディスク）のデータを読むための装置です。

⚠ 注意

装置を安全にお使いいただくために次の注意事項を必ずお守りください。指示を守らないと、火傷やけがなどを負うおそれや物的損害を負うおそれがあります。詳しくは、iiiページ以降の説明をご覧ください。

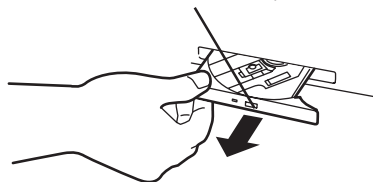
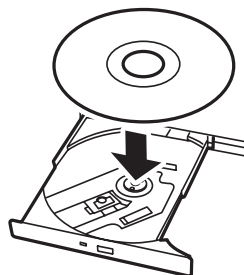
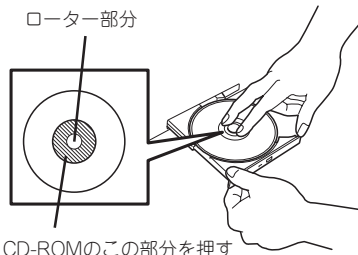
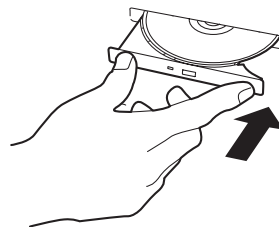
- **CD-ROMドライブのトレーを引き出したまま放置しない**

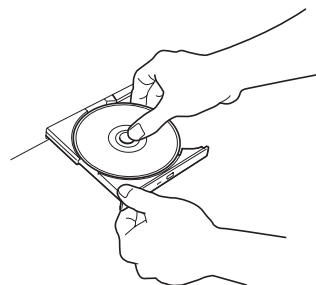
CD-ROMのセット/取り出し

CD-ROMは次の手順でセットします。

1. CD-ROMをCD-ROMドライブにセットする前に本体の電源がON（POWERランプが緑色に点灯）になっていることを確認する。
2. CD-ROMドライブ前面のCDトレーイジェクトボタンを押す。

   トレーが少し出てきます。

3. トレーを軽く持って手前に引き出し、トレーが止まるまで引き出す。
4. CD-ROMの文字が印刷されている面を上にしてトレーの上に静かに、確実に置く。

5. 右図のように片方の手でトレーを持ちながら、もう一方の手でトレーの中心にあるローター部分にCD-ROMの穴がはまるように指で押して、トレーにセットする。

6. トレーの前面を軽く押して元に戻す。

CD-ROMの取り出しは、CD-ROMをセットするときと同じようにCDトレーイジェクトボタンを押してトレーを引き出します。

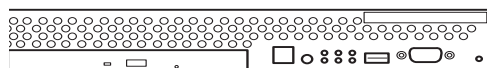
アクセスランプが点灯しているときはCDにアクセスしていることを示します。CDトレーイジェクトボタンを押す前にアクセスランプが点灯していないことを確認してください。

右図のように、片方の手でトレーを持ち、もう一方の手でトレーの中心にあるローター部分を押さえながらCD-ROMの端を軽くつまみ上げるようにしてトレーから取り出します。

CD-ROMを取り出したらトレーを元に戻してください。

CD-ROMが取り出せない場合

CDトレーイジェクトボタンを押してもCD-ROMが取り出せない場合は、次の手順に従ってCD-ROMを取り出します。

1. POWERスイッチを押して本体の電源をOFF(POWERランプ消灯)にする。

2. 直径約1.2mm、長さ約100mmの金属製のピン(太めのゼムクリップを引き伸ばして代用できる)をCD-ROM前面右側にあるエマージェンシーホールに差し込んで、トレーが出てくるまでゆっくりと押す。

エマージェンシーホール

重要

- **つま楊枝やプラスチックなど折れやすいものを使用しないでください。**
- **上記の手順を行ってもCD-ROMが取り出せない場合は、保守サービス会社に連絡してください。**

3. トレーを持って引き出す。

4. CD-ROMを取り出す。

5. トレーを押して元に戻す。

CD-ROMの取り扱いについて

CD-ROMを破損しないように次の点に注意して取り扱ってください。

- CD-ROMを落とさないでください。
- CD-ROMの上にものを置いたり、曲げたりしないでください。
- CD-ROMにラベルなどを貼らないでください。
- 信号面(文字などが印刷されていない面)に手を触れないでください。
- 文字の書かれている面を上にして、トレーにていねいに置いてください。
- キズをつけたり、鉛筆やボールペンで文字などを直接CD-ROMに書き込まないでください。
- たばこの煙の当たるところには置かないでください。
- 直射日光の当たる場所や暖房器具の近くなど温度の高くなる場所には置かないでください。
- 指紋やほこりがついたときは、乾いた柔らかい布で、内側から外側に向けてゆっくり、ていねいにふいてください。
- 清掃の際は、CD専用のクリーナをお使いください。レコード用のスプレー、クリーナ、ベンジン、シンナーなどは使わないでください。
- 使用後は、専用の収納ケースに保管してください。

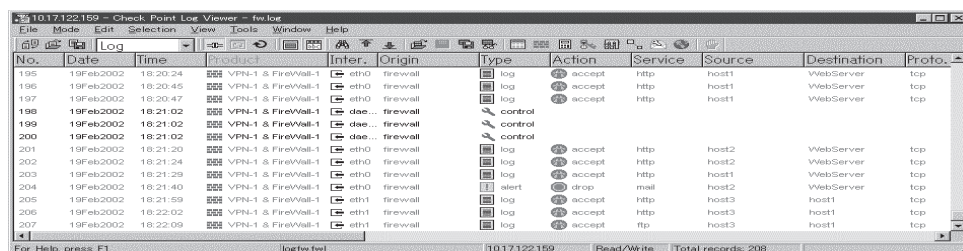
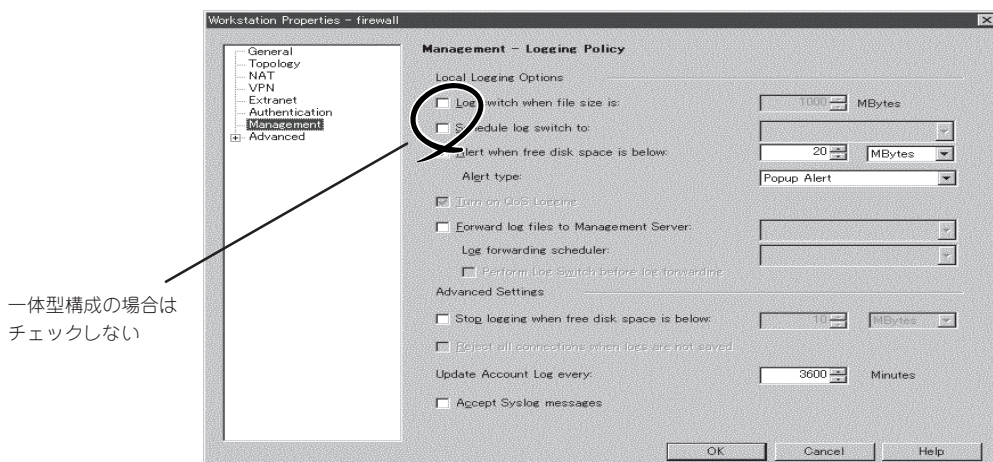
ログの管理

FireWall-1のログは毎日午前4時2分にローテーションされ、基本設定ツールで設定された保存期間だけディスク上に残されます。

FireWall-1のログ領域は、約7GB確保していますが、万一、ファイルシステムがいっぱいになった場合は、過去のログファイルを削除するとともに、基本設定ツールで保存時間を短めに設定し直すようにしてください。

過去のログは以下の形式で /etc/fw/log配下に残っています。

fwlog数字.log
fwlog数字.logptr
fwlog数字.logaccount_ptr
fwlog数字.loginitial_ptr
fwlog数字.adtlog
fwlog数字.adtlogptr
fwlog数字.adtlogaccount_ptr
fwlog数字.adtloginitial_ptr

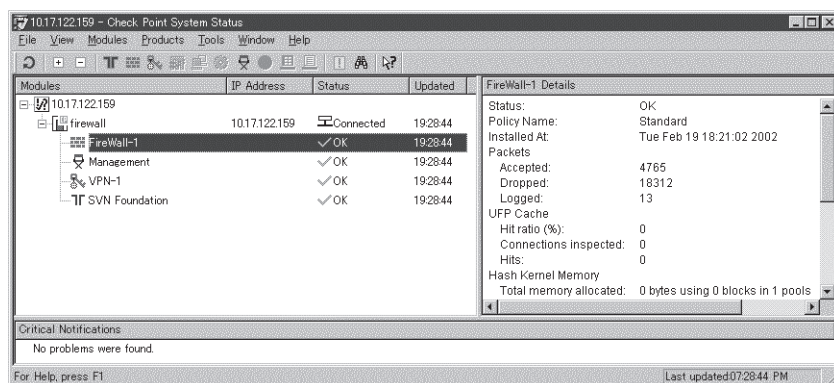
fwlog1.＊が前日のログで、数字が大きいほど過去のログになります。
ログの保存期間を短く設定しなおした場合でも、すでに残っているログファイルを削除することはありませんので、このような場合は、保存期間以上の数字を持つログファイルを必ず削除するようにしてください。

上記のログローテーションは基本設定ツールの機能で行っています。
一体型構成の場合は「Policy Editor」のファイアウォールオブジェクトのプロパティで、自動ログスイッチの機能は使用しないでください。自動ログスイッチにより保存されたログファイルは削除されず、FirewallServerのディスク上に残ってしまいます。

FireWall-1の管理モジュールを別のシステムで運用する分散型構成の場合は、ログはすべて管理モジュールが動作しているシステム上に送られ、サーバ上には残りません。分散型構成の場合は、管理モジュールの動作しているシステムのファイルがいっぱいにならないように注意してください。

ログ内容の確認は、コンソールからFireWall-1のバンドルユーティリティである「Log Viewer」を使って行います。

No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
195	19Feb2002	18:20:24	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host1	WebServer	tcp
196	19Feb2002	18:20:45	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host1	WebServer	tcp
197	19Feb2002	18:20:47	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host1	WebServer	tcp
198	19Feb2002	18:21:02	VPN-1 & FireWall-1	dae...	firewall	control					
199	19Feb2002	18:21:02	VPN-1 & FireWall-1	dae...	firewall	control					
200	19Feb2002	18:21:02	VPN-1 & FireWall-1	dae...	firewall	control					
201	19Feb2002	18:21:20	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host2	WebServer	tcp
202	19Feb2002	18:21:24	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host2	WebServer	tcp
203	19Feb2002	18:21:29	VPN-1 & FireWall-1	eth0	firewall	log	accept	http	host1	WebServer	tcp
204	19Feb2002	18:21:40	VPN-1 & FireWall-1	eth0	firewall	alert	drop	mail	host2	WebServer	tcp
205	19Feb2002	18:21:59	VPN-1 & FireWall-1	eth1	firewall	log	accept	http	host3	host1	tcp
206	19Feb2002	18:22:02	VPN-1 & FireWall-1	eth1	firewall	log	accept	http	host3	host1	tcp
207	19Feb2002	18:22:09	VPN-1 & FireWall-1	eth1	firewall	log	accept	ftp	host3	host1	tcp

Log Viewerは、セットアップの際にインストールすることができます。2章の「セットアップ」を参照してください。Log Viewerの詳細な使用方法については、Check Point Next Generationに付属のマニュアルをご覧ください。

システムステータスのチェック

システムの状態をチェックするユーティリティ「System Status」がFireWall-1にバンドルされています。

システムの障害を未然に防ぐために、「System Status」を使ってコンソールからシステムの状態を定期的にチェックしてください。
System Statusは、セットアップの際にインストールすることができます。2章の「セットアップ」を参照してください。System Statusの詳細な使用方法については、Check Point Next Generationに付属のマニュアルをご覧ください。